IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

UNITED STATES OF AMERICA Plaintiff,	§ § §	
v.	§	NO: 6:23-CV-00351
$1,029,155.26 IN UNITED STATES CURRENCY Defendant.	§ § §	

AFFIDAVIT IN SUPPORT OF COMPLAINT FOR FORFEITURE

I, Brad Schley, after being duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Senior Special Agent (SSA) with the United States Secret Service (USSS) and have been so employed since September 2001. During my tenure with the Secret Service, I have been assigned to investigate violations of federal laws, including violations of Title 18 of the United States Code, specifically those related to the passing of counterfeit United States currency, money laundering, and wire fraud. I received criminal investigative training at the Federal Law Enforcement Training Center in Glynco, Georgia, and at the James J. Rowley Secret Service Training Center in Beltsville, Maryland, pertaining to criminal investigations of counterfeit currency, bank fraud, money laundering, wire fraud, access device fraud, and identity theft. During my employment with the USSS, I have conducted investigations resulting in the arrest of suspects and seizures of criminally derived property. I am an investigative and law

enforcement officer of the United States, in that I am empowered by law to conduct investigations and to make arrests for felony offenses, under authority of 18 U.S.C. § 3056.

2. The statements contained in this affidavit are based in part upon my experience, my knowledge of the facts and circumstances surrounding this investigation, and on information provided to me by other law enforcement personnel and other witnesses.

PROPERTY FOR FORFEITURE

3. This Affidavit is made in support of a civil forfeiture complaint concerning the following personal property:

a. $1,029,155.26 in Wells Fargo Bank accounts 6945288279 (Target Account 1), 2089226720 (Target Account 2), and 9068111294 (Target Account 3), Check No. 0002540888 seized on or about April 6, 2023, in Irving, TX pursuant to a seizure warrant.

LEGAL AUTHORITY FOR FORFEITURE

4. The funds to be forfeited represent proceeds of a computer/technical support fraud scheme. A technical support scheme often begins when victims browse the Internet on electronic devices and receive a "pop-up message" on their device. The "pop-up message" often sounds a loud audible alarm, displays a message that the device was compromised by a computer virus, and instructs the victim to contact a computer technician. Victims report that when the message is visible on their screens, their devices

do not respond to keyboard inputs. Victims state that the "pop-up message" lists telephone numbers by which a technician can be reached. When the victims call the telephone number provided in the "pop-up" message, they are asked to provide their contact information and are informed that a technician will contact them. When the "technician" contacts them, the technician instructs the victim to download remote access software. After the victims download the remote access software, the technician is able to remotely access the victims' devices. Victims report that the technicians indicated various reasons why their computer was compromised, including an "IP address hack" and "computer security issues." Victims report that the technicians offered to provide several different services to ensure that their IP addresses and computers were secured. These services included "Lifetime Lifelock," "Internet Security," and "Microsoft Insurance." Victims were tricked into thinking they were doing business with a legitimate company, such as Microsoft, because the technicians would refer to themselves as Microsoft Technicians or Microsoft-Trained Technicians. Victims report that once the "pop-up messages" were removed, their payments were requested. Victims report that they made payments via checks that were scanned on their computers when the technicians had control of their devices, or that were mailed to various addresses provided by the technicians.

5. I believe the above-listed property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A) because the property was involved in or traceable to property involved in money laundering in violation of 18 U.S.C §§ 1956 or

1957, or constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)).

6. Any property, real or personal, which was involved in a transaction in violation of 18 U.S.C. §§ 1956 or 1957 or any property traceable to such property is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

7. 18 U.S.C. § 1956 (a)(1) makes it a crime to knowingly conduct or attempt to conduct a "financial transaction" with proceeds from "specified unlawful activity" (SUA) with specific intent to: promote the SUA, conceal or disguise the source, origin, nature, ownership, or control of the proceeds; or evade reporting requirements.

8. The purpose of "money laundering" as defined by 18 U.S.C. § 1956 is to disguise illicit nature of funds by introducing it into legitimate commerce and finance thereby making them "clean." This financial process is most commonly conducted using three steps referred to as "placement," "layering," and "integration." Typically, the "placement" phase of this financial process takes place when proceeds from illicit sources are placed in a financial institution or business entity. "Layering" takes place when these funds are then used in seemingly legitimate commerce transactions which makes the tracing of these monies more difficult and removed from the criminal activity from which they are a source. Finally, the "integration" phase is when these funds are then used to promote the unlawful activity or for the personal benefit of the money launderers and others.

9. I also have probable cause to believe that this property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(C) because the property constitutes or is derived from proceeds traceable to violations of 18 U.S.C. § 1343 or a conspiracy to commit such offense.

10. Any property, real or personal, which constitutes proceeds or is derived from proceeds traceable to a violation of 18 U.S.C. § 1343 or a conspiracy to commit such is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

11. Under 18 U.S.C. § 984, for any forfeiture action in rem in which the subject property consists of cash, monetary instruments in bearer form, or funds deposited in an account in a financial institution:

a. The government need not identify the specific funds involved in the offense that serves as the basis for the forfeiture;

b. It is not a defense that those funds have been removed and replaced by other funds; and

c. Identical funds found in the same account as those involved in the offense serving as the basis for the forfeiture are subject to forfeiture.

12. In essence, 18 U.S.C. § 984 allows the government to seize for forfeiture identical property found in the same place where the "guilty" property had been kept.

FACTS SUPPORTING FORFEITURE

13. The United States is investigating a technical support scheme. The investigation concerns possible violations of, inter alia, 18 U.S.C. § 1343 (Wire Fraud), 18 U.S.C. § 1349 (Conspiracy to Commit Wire Fraud) and 18 U.S.C. §§ 1956 and 1957 (Laundering of Monetary Instruments).

14. The case involves the laundering of proceeds obtained from victims of the technical support scheme. Part of the money laundering scheme was to funnel proceeds from the tech fraud scheme through the various business accounts to a finite number of funnel accounts. One business, identified as Red Viking Global LLC, held multiple bank accounts that served as funnel accounts and received fraud proceeds from bank accounts held in the names of the shell companies that received proceeds derived from the technical support scheme.

15. **TARGET ACCOUNT 1** is a business checking account. Bank records show JON TAYLOR[1] as the owner of RED VIKING GLOBAL LLC with a business address of 405 Lexington Ave, New York, New York 10174. As of February 24, 2023, an associated website, www.redvikingglobal.com, stated, "Red Viking Global specializes in structuring and originating loans to individuals and institutions seeking leverage, liquidity, and hedges for publicly-traded securities, mutual funds, equity portfolios, and cryptocurrencies. We customize loans to fit your needs." The website claimed the

[1] JON TAYLOR a/k/a JONATHAN TAYLOR was released from federal prison on April 7, 2020, after serving four years for Sex Trafficking by Force, Fraud, or Coercion.

business had offices in New York, England, China, United Arab Emirates, and Mauritius. The only contact information provided on the website was an email address.

16. The opening documents for **TARGET ACCOUNT 1** state that RED VIKING GLOBAL LLC had six employees and $0 in annual gross sales. From July 14, 2021, through February 9, 2022, $2,399,647.02 was deposited into **TARGET ACCOUNT 1**. From February 10, 2022, through December 31, 2022, the only significant deposit to TARGET ACCOUNT 1 was a $1,000,000 transfer from **TARGET ACCOUNT 2** on April 7, 2022. This transfer was funded entirely by two incoming wire transfers in July 2021 and September 2021 from MKCOGI Water Management in Delhi, India. Open-source checks show MKCOGI Water Management was incorporated in Delhi, India, on February 29, 2016. The listed business activity is collection, purification, and distribution of water. No additional information is known regarding MKCOGI Water Management. As of December 31, 2022, the balance in **TARGET ACCOUNT 1** was $1,335,611.89.

17. From July 2021 through February 2022, there were 67 deposits made into **TARGET ACCOUNT 1** via wire transfer totaling $2,149,431.75. The deposits made via wire transfer included:

Wire Sent By	**Domestic / International**	**Location**	**Number of Wires**	**Total Amount**
JM Vacation Private Limited	International	India	31	$1,218,997.00
Summit Kochar	International	India	1	$204,920.75
Omegainfotek Cloud,	International	Canada	4	$109,920.00

Wire Sent By	Domestic / International	Location	Number of Wires	Total Amount
Inc.				
Workgroup, LLC	Domestic	California	4	$103,150.00
Techisgroup, Inc.	International	Canada	5	$89,400.00
Wisdom Web Online, LLC	Domestic	Pennsylvania	2	$79,350.00
Shiva Logistics, LLC	Domestic	Pennsylvania	2	$49,000.00
AG Maritime Private Limited	International	Singapore	1	$40,000.00
JGJ, LLC	Domestic	Virginia	1	$35,000.00
Webstylers, LLC	Domestic	New Jersey	2	$33,000.00
Element Softnet, Inc.	Domestic	California	2	$30,200.00
YTP Tourism, LLC	International	United Arab Emirates	1	$30,175.00
Holiday Hunger DMC Private Limited	International	India	1	$25,099.00
Sapphire Tech, LLC	Domestic	California	2	$21,000.00
Ran Ventures, LLC	Domestic	Nevada	2	$19,500.00
Divine Tech, LLC	Domestic	New Jersey	1	$15,000.00
Technet Support, LLC	Domestic	Pennsylvania	1	$15,000.00
Jagroop Singh	Domestic	Pennsylvania	1	$10,000.00
Pedro Juan Laboy Molinari	International	Puerto Rico	1	$9,720.00
Web Leaders, Inc.	Domestic	New Jersey	1	$6,000.00
Omegateksol, LLC	Domestic	Massachusetts	1	$5,000.00
Grand Total			**67**	**$2,149,431.75**

18. Complaints have been filed through the FBI's Internet Crime Complaint Center (IC3) alleging computer tech schemes by at least eleven entities that deposited funds into the **TARGET ACCOUNT 1** from July 2021 through October 2021. These entities and the number of associated IC3 complaints are as follows: Technet Support (25), Webstylers (3), Omegateksol (6), Ran Ventures (3), Techisgroup (1), Workgroup

LLC (6), Wisdom Web Online (10), Sapphire Tech (1), Webleaders (7), Divine Tech (22), and Element Softnet (1). There appear to be additional IC3 complaints regarding these companies, but misspellings by complainants, multiple complaints filed by individual victims, and reported name variations make quantification difficult.

19. On or about August 17, 2022, a federal grand jury in the Eastern District of Texas returned an indictment against several individuals who participated in the computer tech scheme. A list of those indicted and the shell companies they operated are identified in the table below:

Defendant	Shell Company
Fnu Ankush **Jenisha Katuwal**	Expert Solutions LLC Shiva Logistics LLC Wisdom Web Online LLC
Sukhwinder Sandhu	Cyber Secure LLC IntellectSoftApps LLC
Inder Pal Singh	Air Ticket Mode LLC Edgenet LLC MS Secure LLC PC Dynamics LLC
Mukul Khanna	Technet Support LLC Webmatrix LLC
Satinder Singh	Commtouch Software LLC Dialogic Support LLC Micron Technology LLC
Ramneek Singh	Neocyber LLC Sigma Works LLC
Muninder Singh	JGJ LLC
Sandeep Heir	Cloudmind Technology LLC
Rachel Mullins **Deepanshu Arora** **Himanshu Arora**	Angel City Transfer
Unindicted Co-Conspirator 1	Live Onecare LLC Surface Web Solutions LLC Worldwide Tradelinks LLC
Unindicted Co-Conspirator 2	Workgroup LLC
Unindicted Co-Conspirator 3	JGJ LLC
Unindicted Co-Conspirator 4	Commtouch Software LLC

20. Paragraph 19 of this affidavit mentions a true bill indictment that was obtained in the Eastern District of Texas on or about August 17, 2022. Based on the investigation in that case, the following victims in the Eastern District of Texas suffered losses as a direct result of a tech support scam.

21. For example, victim TP who resides in the Eastern District of Texas, wrote and mailed approximately 9 checks totaling $23,300.00 to computer tech shell companies

that funneled funds to **Target Account 1**. Between on or about August 26, 2021 and on or about November 8, 2021, the payments sent by TP included:

a. On or about August 26, 2021, victim TP wrote and mailed a check payable to Cyber Secure LLC in the amount of $800.00.

b. On or about September 23, 2021, victim TP wrote and scanned a check payable to Cyber Secure LLC in the amount of $2,500.00.

c. On or about October 7, 2021, victim TP wrote and mailed a check payable to MS Secure LLC in the amount of $2,999.99.

d. On or about October 7, 2021, victim TP wrote and mailed a check payable to Commtouch Software LLC in the amount of $2,800.00.

e. On or about October 19, 2021, victim TP wrote and mailed a check payable to Micron Technology LLC in the amount of $2,596.97.

f. On or about October 19, 2021, victim TP wrote and mailed a check payable to Dialogic Support LLC in the amount of $2,739.86.

g. On or about October 19, 2021, victim TP wrote and mailed a check payable to Commtouch Software LLC in the amount of $2,163.17.

22. Similarly, victim JS who resides in the Eastern District of Texas also suffered a loss due to the technical support scam. JS reported that this scheme caused him/her to write a check in the amount of $199.99. JS stated this check was made payable to Cyber Secure LLC, a computer tech shell company that funneled funds to **Target Account 1**.

23. In April 2022, a law enforcement officer contacted NH, a 77-year-old resident of Richmond, Texas, after analysis indicated that checks written from NH's personal account to Web Leaders and other companies totaled approximately $46,500. NH reported that he wrote checks in excess of $60,000. NH advised that he had been paying for computer services to "clean out viruses" and recalled speaking to technicians from Web Leaders, Webstylers, and another company whose name he could not recall. NH also recalled being told to make payment in gift cards. NH recounted traveling to a Randall's grocery store in Richmond, Texas while on the phone with the technician and being instructed what to say if anyone inquired about his gift card purchases. NH stated he scratched off gift card numbers and provided those numbers as payment. NH stated he last paid for such services in October 2021. NH stated he then realized that he "was being a fool" after he spent "all his savings" on these services.

24. In April 2022, a law enforcement officer interviewed SG, a 65-year-old resident of California. Financial analysis shows that SG has written numerous checks to Web Leaders and other similar companies including Webstylers (the same company referenced by NH), Web Micro Solutions, Webfixers, and Hope Technologies. Altogether, SG has written checks totaling approximately $114,000 to various companies associated with this investigation. SG stated she became concerned that she was being scammed because of the number of checks she had written. Consistent with other victims who paid Web leaders, SG iterated that she often paid the companies by writing out a

check and placing it on the scanner for the technician, who was remotely connected to her computer and scanned the check.

25. Victim PC reported to the FBI that in 2020 or 2021 he found that his computer was frozen, and he had been hacked. A company called Technest told PC they could fix his computer, and he agreed to a multi-year plan. An "accountant" for Technest would virtually log into his computer and type out payment amounts, names, and addresses where PC was to send the funds. PC would take the list to the bank and obtain cashier's checks. He mailed cashier's checks payable to Techis, Digyleap, MS Secure LLC, Surface Web Solutions, Technet Support LLC, Webbloft LLC, Omegateksol, Skyweb IT Services, and Metconnect Inc totaling approximately $370,000.

26. Victim CT reported to IC3 that she received a pop-up message on her computer stating that her computer had been hacked. CT called the number shown and spoke to a purported Apple employee who attempted to sell her computer security. CT eventually agreed to a "clean-up" and was instructed to mail a check to Techisgroup Inc.

27. Victim ER reported that his mother, DT received a pop-up message on her computer stating that it was compromised. DT called a phone number listed on the pop-up message and spoke with someone who sold her a $2,290 subscription for internet security software. DT was instructed to mail a check payable to Omegateksol, and she was also directed to ship $19,800 to an address in Flushing, New York.

28. Victim PL reported to IC3 that a company called Webfixers, LLC contacted her regarding hacking protection in August 2020. Webstylers, LLC took over the

"Hacker Protection" in June 2021, followed by Webleaders, Inc. in September 2021. Each time PL was contacted, she was advised her computer was hacked. She advised that when she hesitated to make additional payments, she was shown her social security number to make her fear that she had been the victim of identity fraud. From August 27, 2020, through November 29, 2021, PL sent 10 cashier's checks totaling approximately $11,000. Valley Bank received three of the cashier's checks paid to Webleaders, Inc. The wire transfer deposited on August 27, 2021, into **TARGET ACCOUNT 1** from Webleaders, Inc. originated at Valley Bank.

29. From December 2019 through February 2022, at least ten complaints were filed with IC3 regarding Wisdom Web Online LLC. Victims reported being defrauded by tech support schemes after receiving pop-up messages on their computers. Victim GS reported sending cashier's checks payable to Wisdom Web Online LLC, MS Secure LLC, Workgroup LLC, and ESharp Systems LLC.

30. Victim MS reported to the Pine Creek Township Pennsylvania Police Department that in January 2021, her computer froze, and she received a message from Web Support Solutions. MS called the number on the screen and was told her computer could be fixed if she provided remote access. Once the repair service was complete, Web Support Solutions told MS she owed them $11,436. MS wrote checks to Digyleap for the remote repair of her computer. Between January 2021 and November 2022, IC3 received at least 15 complaints regarding Digyleap for computer technical support fraud. In July 2021, MS was contacted by Divine Tech, who advised her that the invoice for fixing her

computer had not been paid in full. MS subsequently wrote five checks totaling $21,198.12 to Divine Tech.

31. Victim JM reported to IC3 that in 2019, she began paying Infotech Solutions for security on her computer. She was subsequently offered lifetime computer security, for which she paid $10,380.60. She was instructed to call Infotech Solutions every month for a check-up. In 2020, she was told her computer had been hacked and she would need to pay Infotech Solutions $8,155. An Infotech Solutions employee asked JM how much money she had in her bank account, and she realized she had been scammed.

32. Victim KG reported to IC3 that he was the victim of a computer intrusion in late 2020. In order to have the computer fixed, KG was advised by Technest Solutions that he would have to mail a check for $4,994 to Element Softnet, 2010-A Harbison Drive, #457, Vacaville, California. KG realized he had been scammed and stopped payment on the check. However, representatives from Element Softnet continued contacting him for months. On October 7, 2021, and October 21, 2021, two wires for $15,100 each from Element Softnet were deposited into **TARGET ACCOUNT 1**. The address shown on bank records for Element Softnet was 2010-A Harbison Drive, #457, Vacaville, California.

33. Victim GS reported to IC3 that between May 2020 and October 2021, he was victimized by a computer technical support scam. As a result, GS sent 53 checks totaling more than $115,000 to various locations at the direction of the scammers,

including to MS Secure LLC, Workgroup LLC, ESharp Systems LLC, and Wisdom Web Online at 1712 S. 7th Street, Philadelphia, Pennsylvania, the same address used by Shiva Logistics.

34. Shiva Logistics was registered as a transportation company in Pennsylvania on February 25, 2021. **TARGET ACCOUNT 1** received wire transfers from Shiva Logistics on July 15, 2021, and July 20, 2021 totaling $49,000. The reported owner of Shiva Logistics is Jenisha Katuwal.[2]

Additional wire transfers identified.

35. A wire transfer deposited into **TARGET ACCOUNT 1** from Webstylers, LLC on July 20, 2021, in the amount of $23,000 originated from Columbia Bank account ending in 0736. Webstylers LLC is the target of an FBI Newark investigation wherein victims are convinced their computers have a virus and offer to repair the computer for a fee. Investigators have identified more than 100 deposits made into account ending in 0736 by fraud victims, including by WGL, who also deposited funds into another account uncovered in this investigation.

36. On July 21, 2021, a $5,500 wire transfer from Ran Ventures LLC, 5470 Kietzke Lane, Suite 300, Reno, Nevada, was deposited into **TARGET ACCOUNT 1**. Between March 2021 and October 2022, at least three complaints were filed with IC3 regarding Ran Ventures. All three of these complaints involved victims whose

[2] Jenisha Katuwal is a defendant under indictment in 6:22-CR-111 for violating 18 U.S.C § 1349.

computers were remotely accessed in a tech support fraud scheme. The victims reported sending checks to Ran Ventures, 5470 Kietzke Lane, Suite 300, Reno, Nevada, the same address used with victims PC and DT.

37. On August 4, 2021, a $35,500 wire transfer from Workgroup LLC was deposited into **TARGET ACCOUNT 1**. From April 2020 through February 2022, at least six complaints were filed with IC3 regarding Workgroup LLC. All six victims reported being defrauded through tech support schemes after pop-up messages appeared on their computers. Victim JR reported sending checks totaling $21,901.16 payable to Workgroup LLC, NeoCyber LLC, CommTouch Software LLC, Sigma Workforce LLC, Cyber Secure LLC, and MS Secure LLC from June 2, 2021, through August 11, 2021.

38. On August 18, 2021, and August 27, 2021, wire transfers for $15,000 and $6,000 respectively, from Sapphire Tech LLC were deposited into **TARGET ACCOUNT 1**.

39. From July 2021 through February 2022, **TARGET ACCOUNT 1** received $605,520.00 of confirmed fraud proceeds from shell companies that received victim funds of computer tech fraud schemes.

Target account 2 transaction activity.

40. On July 21, 2021, **TARGET ACCOUNT 2** was opened with a $1,000 deposit in the name of RED VIKING GLOBAL LLC. JON TAYLOR was the sole owner. The account opening documents claimed that RED VIKING GLOBAL LLC had two employees and $3,000,000 in annual gross sales, although no banking activity in

support of such sales was observed in any of the **TARGET ACCOUNTS** prior to July 2021. Under "Description of Business", the opening documents state, "Consults with debts and entities (sp) overseas." Open-source documents also show that RED VIKING GLOBAL LLC was registered as a Florida business on July 21, 2021, although it was previously registered as a Wyoming business on May 27, 2020, shortly before **TARGET ACCOUNT 1** was opened on July 24, 2020.

41. On July 29, 2021, **TARGET ACCOUNT 2** received a $1,892,606.36 wire transfer from MKCOGI Water Management in Delhi, India. The note associated with the wire transfer states, "ODI Under Equity Purchase." On September 28, 2021, **TARGET ACCOUNT 2** received a $228,450 wire transfer from MKCOGI Water Management in Delhi, India. The note associated with the wire transfer also states, "ODI Under Equity Purchase." From June 1, 2022, through December 1, 2022, $34,000 was transferred from **TARGET ACCOUNT 1** to **TARGET ACCOUNT 2**. No other significant deposits were made to **TARGET ACCOUNT 2**.

42. On April 7, 2022, a $1,000,000 transfer from **TARGET ACCOUNT 2** was made to **TARGET ACCOUNT 1**.

43. **TARGET ACCOUNT 3** was opened in the name of JON TAYLOR on May 8, 2020. On July 8, 2021, the balance in **TARGET ACCOUNT 3** was $1.44. From July 2021 through November 2022, TARGET ACCOUNT 3 received the following transfers:

Date	Amount	Source Account
7/15/2021	$10,000.00	**TARGET ACCOUNT 1**
7/16/2021	$20,000.00	**TARGET ACCOUNT 1**
7/22/2021	$47,000.00	**TARGET ACCOUNT 1**
7/30/2021	$200,000.00	**TARGET ACCOUNT 2**
8/2/2021	$200,000.00	**TARGET ACCOUNT 2**
8/10/2021	$88,000.00	**TARGET ACCOUNT 1**
8/23/2021	$93,000.00	**TARGET ACCOUNT 2**
8/23/2021	$97,000.00	**TARGET ACCOUNT 1**
9/24/2021	$150,000.00	**TARGET ACCOUNT 1**
9/24/2021	$300,000.00	**TARGET ACCOUNT 2**
5/12/2022	$130,000.00	**TARGET ACCOUNT 2**
8/23/2022	$240,000.00	**TARGET ACCOUNT 1**
11/17/2022	$35,000.00	**TARGET ACCOUNT 1**

44. As of January 9, 2023, the balance in **TARGET ACCOUNT 3** was $41,827.36. As shown above, **TARGET ACCOUNT 3** is nearly entirely funded by **TARGET ACCOUNT 1** and **TARGET ACCOUNT 2**.

CONCLUSION

45. I submit that this affidavit supports probable cause for a warrant to forfeit all funds, monies, and other things of value up to $1,029,155.26 seized from Wells Fargo Bank accounts 6945288279, 2089226720 and 9068111294 .

46. Based on my experience and the information herein, I have probable cause to believe that the seized $1,029,155.26 constitutes proceeds from a specified unlawful activity (as defined in 18 U.S.C. § 1956(c)(7) and 18 U.S.C. § 1961(1)), are traceable to a money laundering transaction and are therefore subject to forfeiture pursuant to pursuant to 18 U.S.C. § 981(a)(1)(A).

47. I also have probable cause to believe that the seized $$1,029,155.26 constitutes proceeds traceable to a violation of 18 U.S.C. § 1343 and/or 18 U.S.C. § 1349, and are therefore is subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(C).

As provided in 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Brad Schley

Brad Schley, Special Agent
U.S. Secret Service